

**SECURITY FRAMEWORK FOR IP MOBILITY SYSTEMS
USING VARIABLE-BASED SECURITY ASSOCIATIONS
AND BROKER REDIRECTION**

ABSTRACT

In an IP-based mobile communications system, the Mobile Node changes its point of attachment to the network while maintaining network connectivity. Security concerns arise in the mobile system because authorized users are subject to the following forms of attack: (1) session stealing where a hostile node hijacks session from mobile node by redirecting packets, (2) spoofing where the identity of an authorized user is utilized in an unauthorized manner to obtain access to the network, and (3) eavesdropping and stealing of data during session with authorized user. No separate secure network exists in the IP-based mobility communications system, and therefore, it is necessary to protect information transmitted in the mobile system from the above-identified security attacks.

The present invention improves the security of communications in a IP mobile communications system by creating variable-based Security Associations between various nodes on the system, a Virtual Private Network supported by an Service Level Agreement between various foreign networks and a home network, and an SLA Broker to promote large-scale roaming among different SLAs supported by the SLA Broker or agreements with other SLA Brokers.

009790-059560